CLAIMS

1. A method of processing data (LECM1), encrypted according to an encryption method specific to a first domain such that they cannot be decrypted without the aid of a first secret (K_{N1}) specific to said first domain, said data being received in a presentation device (202) connected to a network belonging to a second domain, characterized in that it comprises the steps consisting, for the presentation device, in:

(a) transmitting (404) to a processing device (211) connected to the network at least a portion ($E\{K_{N1}\}(K_C)$) of said encrypted data;

(b) receiving (408) from said processing device (211) at least one element ($E\{K_{N2}\}(K'_C)|E\{K'_C\}(K_C)$) being used to decrypt said received data with the aid of a second secret (K_{N2}) specific to said second domain, said second secret being contained in the presentation device.

2. The method as claimed in claim 1, characterized in that the data received in the presentation device (202) are encrypted with the aid of a first symmetric key (K_C), said first symmetric key being received with said data in a form encrypted ($E\{K_{N1}\}(K_C)$) with the aid of the first secret (K_{N1});

in that step (a) consists in transmitting to the processing device the first symmetric key encrypted ($E\{K_{N1}\}(K_C)$) with the aid of the first secret; and

in that step (b) consists in receiving from the processing device:

- said first symmetric key encrypted ($E\{K'_C\}(K_C)$) with the aid of a second symmetric key (K'_C); and
- the second symmetric key encrypted ($E\{K_{N2}\}(K'_C)$) with the aid of the second secret (K_{N2}) specific to the second domain.

3. The method as claimed in claim 2, characterized in that it also comprises the steps consisting, for the presentation device, in:

(c) decrypting (409), with the aid of the second secret (K_{N2}), the second encrypted symmetric key (K'_C);

(d) decrypting (410), with the aid of the second symmetric key (K'_C), the first encrypted symmetric key (K_C); and

(e) decrypting the data received (LECM1) by said presentation device with the aid of the first symmetric key (K_C).

4. The method as claimed in claim 3, characterized in that it also comprises, before step (a), a step (403) consisting, for the presentation device, in generating a random number (R),

said random number (R) being transmitted to the processing device, in step (a), with the encryption ($E\{K_{N1}\}(K_C)$) of the first symmetric key;

and in that the data received in step (b) contain a random number (R) and the first symmetric key (K_C) encrypted ($E\{K'_C\}(R|K_C)$) with the aid of the second symmetric key (K'_C);

step (d) also comprising the decryption, with the aid of the second symmetric (K'_C), of the encrypted random number (R) received in step (b); and

the method also comprising, before step (e), a verification step (411) to verify that the random number (R) decrypted in step (d) is identical to the random number (R) generated before step (a); step (e) being performed only in the event of positive verification.

5. The method as claimed in one of the preceding claims, characterized in that a domain identifier (ID_{N1}) is contained in the data (LECM1) received by the presentation device (202) and

in that said domain identifier is transmitted to the processing device (211) during step (a);

step (b) being performed only if said processing device contains the same domain identifier.